PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04L 29/06, 9/08, 12/58

A3

(11) International Publication Number: WO 00/18060

(43) International Publication Date: 30 March 2000 (30.03.00)

(21) International Application Number: PCT/GB99/03140

(22) International Filing Date: 21 September 1999 (21.09.99)

(30) Priority Data:
9820558.6 21 September 1998 (21.09.98) GB

(71) Applicant *(for all designated States except US)*: THE POST OFFICE [GB/GB]; Royal Mail House, 148 Old Street, London EC1V 9HQ (GB).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: PERKINS, Rodney [GB/GB]; 11 Pennine View, Heage, Belper, Derbyshire DE56 2TE (GB).

(74) Agents: KINSLER, Maureen, Catherine et al.; Kilburn & Strode, 20 Red Lion Street, London WC1R 4PJ (GB).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

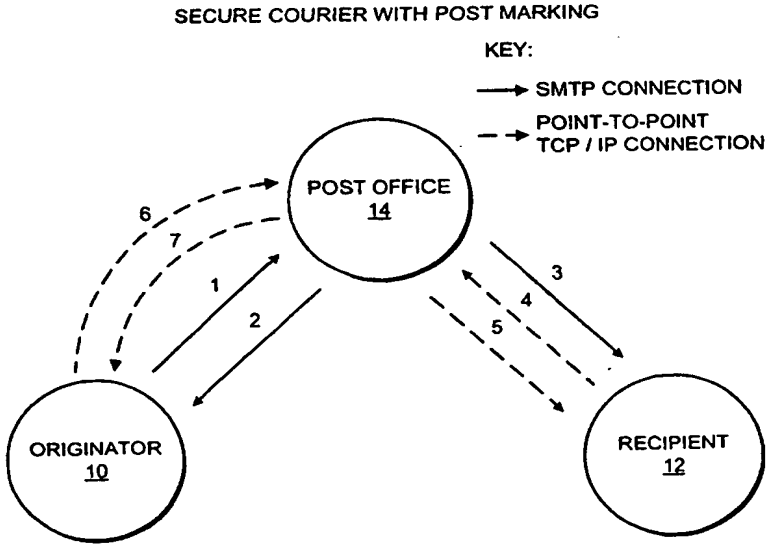
Published
With international search report.

(88) Date of publication of the international search report:
8 June 2000 (08.06.00)

(54) Title: A SECURE DATA TRANSFER SYSTEM

(57) Abstract

A data transfer system comprises a sender (10), receiver (12) and a key facility (14). The sender (10) encrypts data and splits it into parts. One part is further encrypted for a key facility (14). The parts are sent (3) to the receiver (12). The receiver (12) requests (4) decryption of the part encrypted for the facility and the receiver (12) is then able to decrypt the complete data.



1: MESSAGE SENT FROM POST OFFICE
2: POST OFFICE RETURNS PROOF-OF-SUBMISSION
3: POST OFFICE DELIVERS MESSAGE
4: RECIPIENT REQUESTS THE KEY TO DECIPHER THE MESSAGE
5: POST OFFICE LOGS THE REQUEST AND RETURNS THE KEY
6: ORIGINATOR QUERIES THE STATUS OF THE MESSAGE
7: POST OFFICE RETURNS RESPONSE TO THE ORIGINATORS' QUERY

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Assurances as to the identity of the decrypter, i.e. the recipient, are just as necessary as those associated with the encrypter. To address this it is known to employ the services of a trusted third party (TTP) or certificate authority. The role of the TTP is to certify to either or both parties that the other is who they purport to be. Certification links a particular key with the identity of a party. Clearly, the security of the TTP is vital to its standing as an issuer of certificates.

The certificate typically includes identification data as well as identification of the certification authority and the duration for which the certificate is valid. A so-called distinguished name provides authentication of an identity linked to a specific capacity, e.g. rank in an organisational hierarchy. This can be used in addition to the certificate associated with the transacting site.

Encryption software enables users to communicate securely by encrypting files and attaching them to electronic mail (e-mail) messages. The files cannot be read by anybody other than the intended recipient of proven identity.

There is a need for an electronic equivalent of the recorded and registered postal systems. In many instances, it is necessary for the sender of mail at least to have verification that it has been received by the authorised recipient (proof of delivery). A recorded postal letter is signed for by the recipient when it is handed over by the deliverer. A registered postal letter is tracked through the postal system and logged as having passed various points up to delivery.

In an e-mail system the verification of delivery is not necessarily assured because either the acknowledgement software of the recipient may be disabled

or the recipient is posing as the intended recipient fraudulently. E-mail is not inherently secure. Thus, security of an e-mail message depends entirely upon encryption of the message and the encryption system remaining uncompromised.

It has been proposed that recorded e-mail delivery can be effected by using an encryption system by which an encrypted message is transferred to, and held by, a central point associated with a TTP for onward delivery to an authenticated user. The message is stored at the TTP until it is requested by the intended recipient in response to notification that the message is waiting. However, it has been found that there is a practical limit on the amount of information the TTP can store. Thus, the system is dependent upon the storage capacity of the TTP. Furthermore, not only the encryption system but the message itself has to conform to the TTP's reception/transmission system both in terms of format and transmission medium.

According to the present invention there is provided a data transfer system comprising: a sender facility; a receiver facility and a key facility; the sender facility having means for encrypting data for the intended recipient, means for splitting the data into encrypted parts such that no part is decrypted on its own, means for encrypting at least one of the parts for a third party to produce a further encrypted part, means for combining the further encrypted part and the remaining encrypted part to produce a data block and means for sending the data block, the receiver facility having means for receiving the data block, means for requesting decryption of the further encrypted part by the key facility which has means for decrypting the further encrypted part and means for sending it to the receiver facility and the receiver facility also having means for

PKCS#7 mode. The Entrust security system has various architecture components. The security is based on a choice of symmetric key algorithm, including the Data Encryption Standard (DES), Triple DES and CAST; asymmetric or public key algorithms, such a RSA, DSA and DIFFIE HELLMAN; and hashing algorithms such as SHA-1, MD2 and MD5. These are only examples of key systems. Other key systems will be known to the skilled person which could be used to equal effect. The receiver and TTP sites are similarly provided with Entrust System components configured to receive and decrypt data sent by the sender as described below.

Referring to Figure 4a, at the sender site 10 the plain text message P/T is both encrypted with the public key for the recipient or a group of recipients and signed by the PEM method using the sender's private key. The 'header' part of the message is split off, i.e. in the standard PEM format that part from "-----BEGIN PRIVACY-ENHANCED MESSAGE-----" to the terminating empty line. This is referred to as the "inner header" 22. The remainder is the "encrypted text" 20.

Referring to Figure 4b), still at the sender site 10, the inner header 22 is further encrypted and signed by the PEM method using the public key of the third party only. This produces an "encrypted header" 24 and an "outer header" 26. The encrypted text 20, encrypted inner header 24 and outer header 26 are combined and digitally signed (signature 27). The Message Integrity Check (MIC) field of the Outer Header 26 is a convenient unique identifier as it is a hash of the inner header 22 which, in turn, contains a hash of the plaintext; so the outer header MIC is dependent on the contents of the plaintext. Also, the inner header varies even when the same plaintext is used as the symmetric key is

chosen at random on each occasion.

The encrypted text 20, encrypted inner header 24, the outer header 26 and signature 27 are sent as a multi-purpose internet mail extension (MIME) within an e-mail message to form a message package. The unencrypted body of the message itself is an explanation of the sent data and instructions to the recipient on how to obtain software to decrypt the MIME inclusion.

The sender (and recipient) software for preparing the encrypted data comprises Microsoft Exchange or Outlook management software as well as the new plug-in interface. The preparation of the message is Windows-based, providing a tool bar button to click on if the service is required for encrypting e-mail transmission.

This embodiment of the invention is a form of e-mail recorded delivery. Thus, the prepared secure message is sent by the SMTP connection to the receiver site directly. At the same time an alerting message may be sent from the sender site to the TTP. Upon receipt of the e-mail message package the recipient is presented with the open e-mail message containing the instructions, the cipher text, the encrypted header, the outer header intended for the TTP. The recipient's software extracts the inner and outer headers, signs them as one block using PEM or PKCS#7 and transmits them to the TTP using TCP/IP. Thus, the receiver site is instructed by the open e-mail message to send at least the encrypted header 24 and the outer header 26 to the TTP, as indicated in Figure 4c, as a request for decryption of the encrypted header.

At the TTP the signature is checked. This process reveals the identity of the

CLAIMS:

1. A data transfer system comprising: a sender facility; a receiver facility and a key facility; the sender facility having means for encrypting data for the intended recipient. means for splitting the data into encrypted parts such that no part is decryptable on its own, means for encrypting at least one of the parts for a third party to produce a further encrypted part. means for combining the further encrypted part and the remaining encrypted part to produce a data block and means for sending the data block. the receiver facility having means for receiving the data block, means for requesting decryption of the further encrypted part by the key facility which has means for decrypting the further encrypted part and means for sending it to the receiver facility and the receiver facility also having means for decrypting the encrypted part and the decrypted further encrypted part provided by the key facility.

2. A system as claimed in claim 1 in which the sender facility includes means for signing the data block.

3. A system as claimed in claim 1 or 2 in which the means for sending at the sender facility are arranged to send the data block to the key facility and the key facility includes means for receiving the data block and forwarding the said block to the receiver facility.

4. A system as claimed in claim 3 in which the key facility further includes means for logging receipt of the data block.

5. A system as claimed in claim 1 or 2 in which the means for sending at the sender facility are arranged to send the data block to the receiver facility and the receiver facility includes means for receiving the data block.

6. A system as claimed in claim 5 in which the key facility further includes means for logging receipt of the further encrypted part.

7. A system as claimed in any of claims 1 to 6 in which the key facility includes means for logging receipt of the request for decryption of the further encrypted part as proof of delivery of the block to the receiver facility.

8. A system as claimed in claim 7 in which the sender facility includes means for requesting proof of delivery information from the key facility.

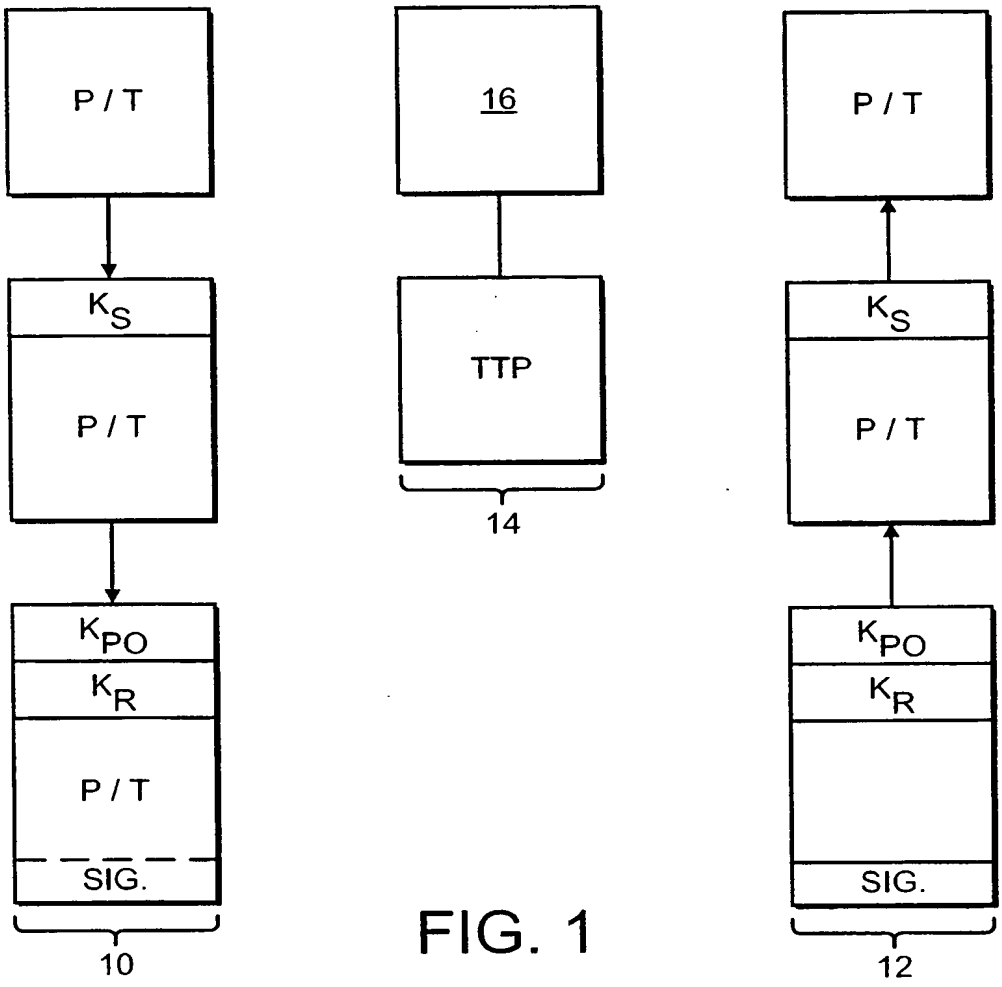
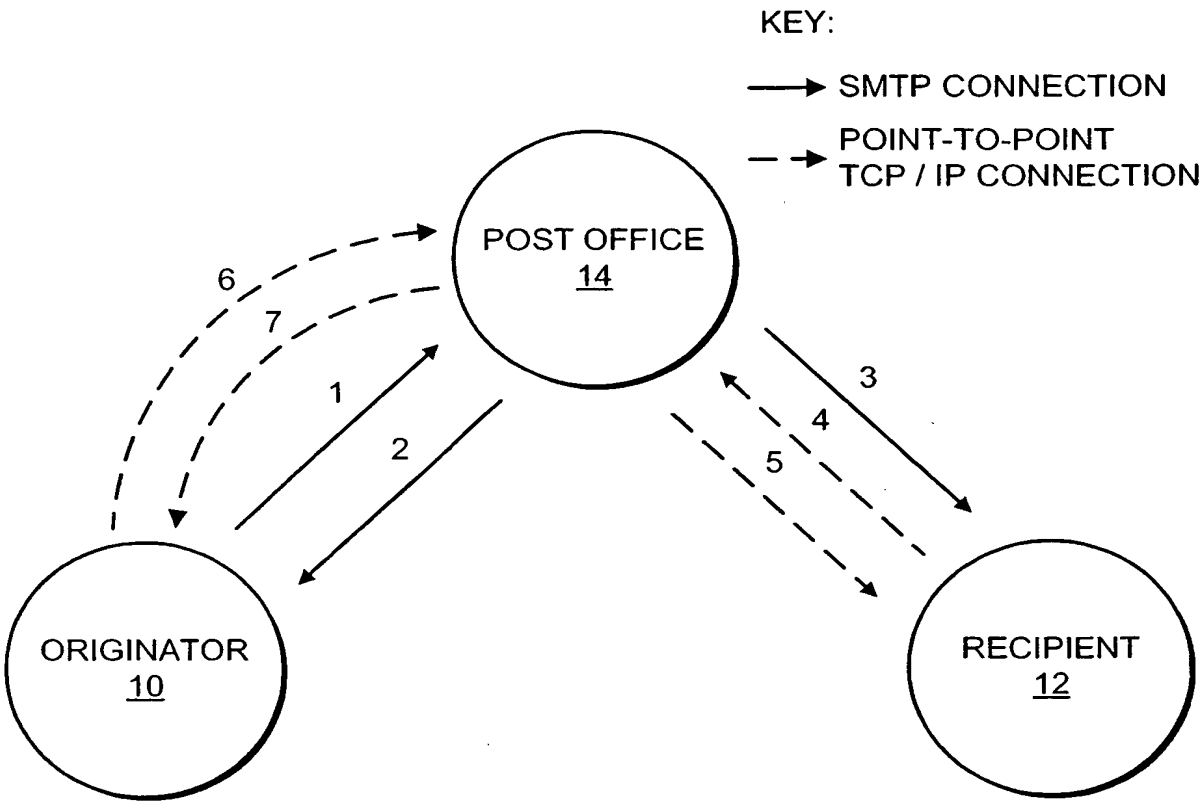


FIG. 1

FIG. 2

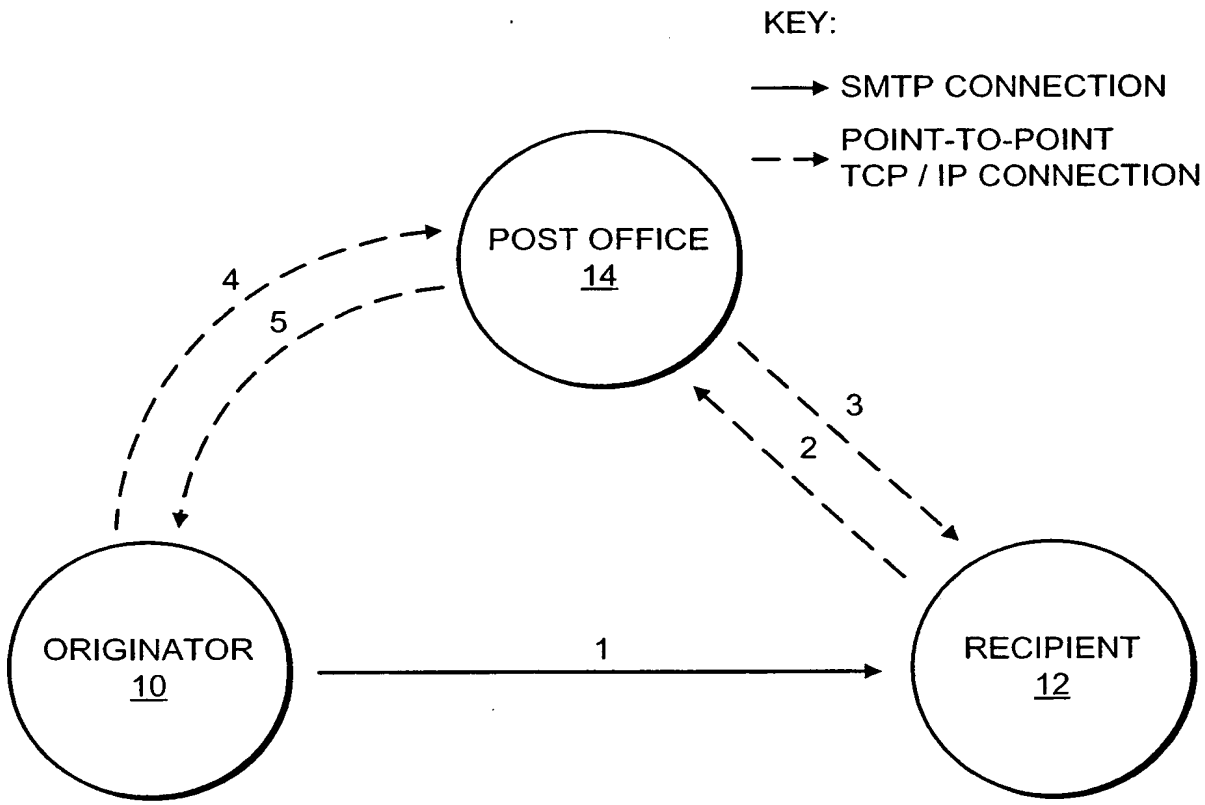
SECURE COURIER WITH POST MARKING



1: MESSAGE SENT FROM POST OFFICE
2: POST OFFICE RETURNS PROOF-OF-SUBMISSION
3: POST OFFICE DELIVERS MESSAGE
4: RECIPIENT REQUESTS THE KEY TO DECIPHER THE MESSAGE
5: POST OFFICE LOGS THE REQUEST AND RETURNS THE KEY
6: ORIGINATOR QUERIES THE STATUS OF THE MESSAGE
7: POST OFFICE RETURNS RESPONSE TO THE ORIGINATORS' QUERY

FIG. 3

SECURE COURIER WITHOUT POST MARKING



1: MESSAGE SENT FROM ORIGINATOR TO RECIPIENT
2: RECIPIENT REQUESTS THE KEY TO DECIPHER THE MESSAGE
3: POST OFFICE LOGS THE REQUEST AND RETURNS THE KEY
4: ORIGINATOR QUERIES THE STATUS OF THE MESSAGE
5: POST OFFICE RETURNS RESPONSE TO THE ORIGINATORS' QUERY

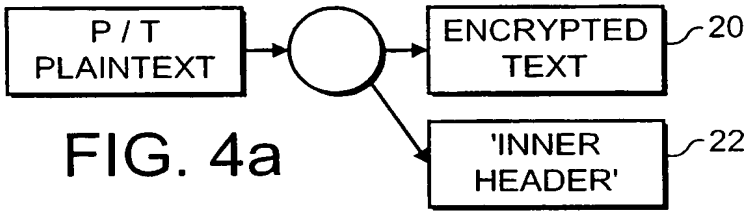


FIG. 4a

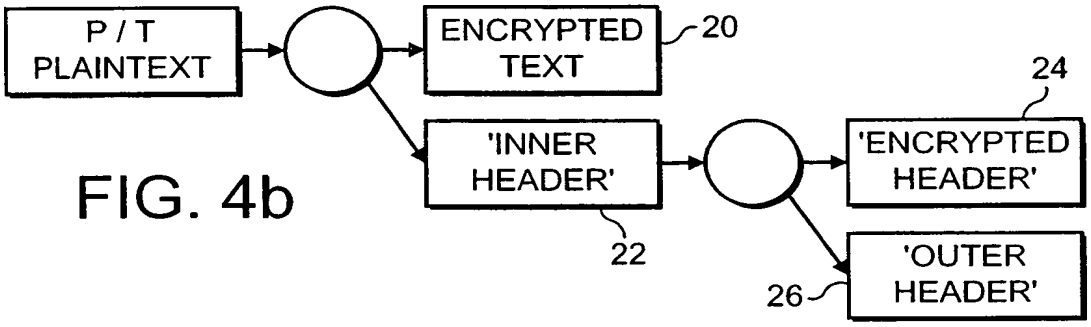


FIG. 4b

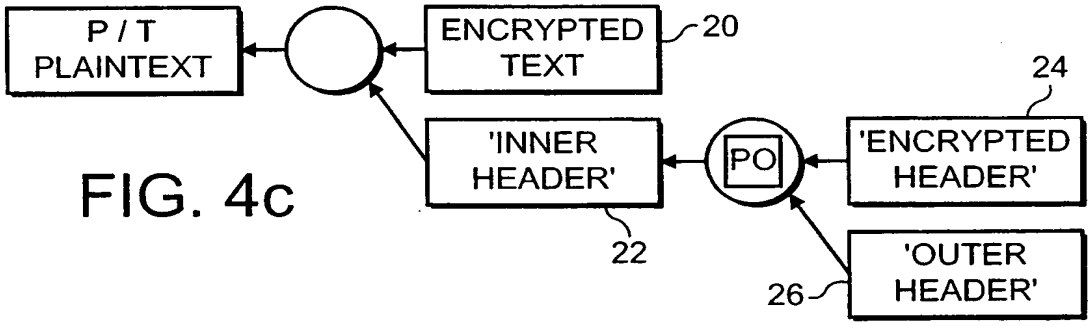


FIG. 4c

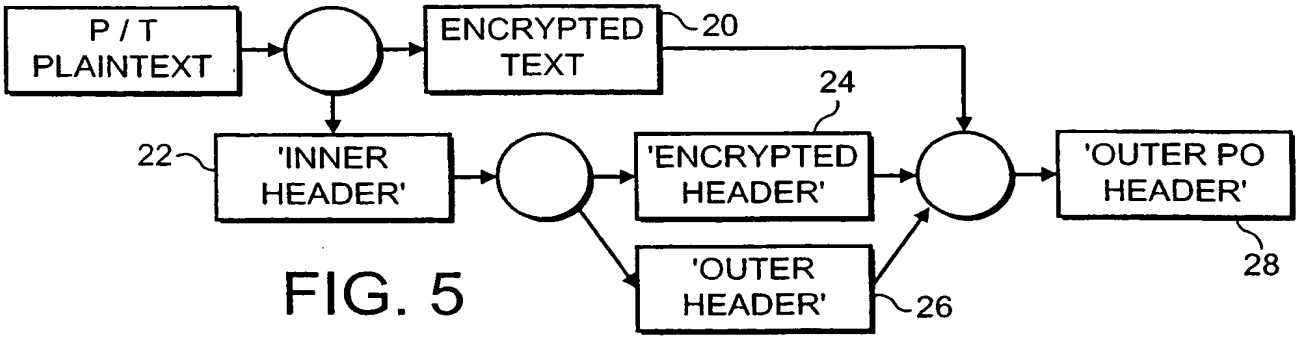


FIG. 5

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 99/03140

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L9/08 H04L12/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 798 892 A (IBM) 1 October 1997 (1997-10-01) column 3, line 5-16	1
A	US 5 557 765 A (ELLISON CARL M ET AL) 17 September 1996 (1996-09-17) column 6, line 1-60 column 15, line 33 -column 16, line 5	1
A	J. LINN: "Privacy Enhancement for Internet Electronic Mail: Part 1: Message Encryption and authentication procedures" RFC1421, 'Online! February 1993 (1993-02), pages 6-30, XP002132590 Retrieved from the Internet: <URL:ftp://ftp.isi.edu/in-notes/rfc1421.txt> 'retrieved on 2000-03-09! the whole document	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 March 2000	24/03/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Dupuis, H

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 99/03140

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0798892 A	01-10-1997	US 5673316 A	30-09-1997
		JP 10040100 A	13-02-1998
US 5557765 A	17-09-1996	US 5557346 A	17-09-1996
		AU 3321795 A	07-03-1996
		BR 9508548 A	03-11-1998
		CA 2197206 A	22-02-1996
		CN 1158195 A	27-08-1997
		EP 0775401 A	28-05-1997
		JP 10508438 T	18-08-1998
		US 5991406 A	23-11-1999
		WO 9605673 A	22-02-1996
		US 5745573 A	28-04-1998
		US 5640454 A	17-06-1997
		US 5956403 A	21-09-1999